



## PRIVACY MANAGEMENT PLAN

<b>Date first approved:</b> 7 December 2012	<b>Date of effect:</b> 7 December 2012	<b>Date last amended:</b> 31 March 2023	<b>Date of Next Review:</b> 23 May 2024
<b>First Approved by:</b>	University Council		
<b>Custodian title &amp; e-mail address:</b>	General Counsel <a href="mailto:privacy-enquiry@uow.edu.au">privacy-enquiry@uow.edu.au</a>		
<b>Author:</b>	Director, Governance and Legal Division		
<b>Responsible Division &amp; Unit:</b>	Office of General Counsel, Information Compliance Unit		
<b>Supporting documents, procedures &amp; forms of this procedure:</b>	<a href="#">Privacy Policy</a> <a href="#">University Code of Conduct</a> <a href="#">Privacy Complaint Internal Review Application Form</a> <a href="#">Data Breach Response Plan</a> <a href="#">Privacy Impact Assessment (PIA) Tool</a> <a href="#">IT Acceptable Use Policy</a> <a href="#">Cybersecurity Policy</a> <a href="#">Records Management Policy</a> <a href="#">University Code of Conduct</a> <a href="#">Fraud and Corruption Prevention Policy</a> <a href="#">Workplace Health and Safety Policy</a>		
<b>Relevant Legislation &amp; External Documents:</b>	<a href="#">Privacy and Personal Information Protection Act 1998 (NSW) (“PPIPA”)</a> <a href="#">Health Records and Information Privacy Act 2002 (NSW) (“HRIPA”)</a> <a href="#">Information and Privacy Commission NSW</a> <a href="#">Government Information (Public Access) Act 2009 (NSW)</a> <a href="#">Independent Commission Against Corruption Act 1988 (NSW)</a> <a href="#">Public Interest Disclosures Act 1994 (NSW)</a> <a href="#">State Records Act 1998 (NSW)</a> <a href="#">Workplace Surveillance Act 2005 (NSW)</a> <a href="#">Work Health and Safety Act 2011 (NSW)</a> <a href="#">Privacy Act 1988 (Cth)</a> <a href="#">General Data Protection Regulation (EU)</a> <a href="#">University of Wollongong Act 1989 (NSW)</a> <a href="#">University of Wollongong By Law 2005 (NSW)</a> <a href="#">Rules of the University of Wollongong</a> <a href="#">Higher Education Support Act 2003 (Cth)</a> <a href="#">Health Practitioner Regulation National Law 2009 (NSW)</a> <a href="#">Anti-Discrimination Act 1977 (NSW)</a> <a href="#">Disability Discrimination Act 1992 (Cth)</a>		
<b>Audience:</b>	Public		



## Table of Contents

<b>A. Privacy management plan overview .....</b>	<b>4</b>
1 Introduction / Background .....	4
2 Purpose.....	4
3 Definitions.....	5
4 The Information Protection Principles and Health Privacy Principles .....	6
<b>B. Collection of Information.....</b>	<b>7</b>
5 UOW must collect information for lawful purposes.....	7
6 How UOW determines the lawful purposes of collection .....	7
7 UOW must collect Information directly from the individual.....	8
8 How UOW collects Information directly from the individual .....	8
9 Indirect collection of Information.....	9
10 UOW must be open and transparent about the handling of Information .....	9
11 UOW’s use of Privacy Statements.....	10
12 UOW must ensure that Information collected is relevant to its lawful purpose .....	11
<b>C. Management of Information by UOW .....</b>	<b>11</b>
13 UOW must ensure security of Information.....	11
14 UOW’s commitment to protecting Information.....	12
15 UOW’s recordkeeping obligations.....	12
16 UOW must check accuracy of Information before use .....	13
17 How UOW ensures accuracy of Information before use .....	13
18 Use and Disclosure of Personal Information .....	13
19 How UOW applies the use and disclosure principles of Personal information .....	14
20 Use and Disclosure of Health Information.....	17
21 How UOW applies the use and disclosure principles of Health information .....	18
22 Other Health Privacy Principles.....	19



23	Third Party Engagement and Confidentiality .....	20
24	Public Registers Held by UOW .....	21
<b>D.</b>	<b>Rights to access/amend Information held by UOW .....</b>	<b>21</b>
25	Access to Information Held by UOW .....	21
26	How Information can be accessed from UOW .....	21
27	Alteration of Information held by UOW .....	22
28	How UOW handles requests for amendments to Information .....	23
<b>E.</b>	<b>Rights to raise concerns and/or make complaints .....</b>	<b>23</b>
29	Complaints and/or Internal Reviews .....	23
30	The Internal Review process .....	24
31	How to lodge an appeal of UOW's Internal Review decision .....	25
<b>F.</b>	<b>Application of other privacy laws .....</b>	<b>26</b>
32	Application of Commonwealth Privacy Act .....	26
33	Application of General Data Protection Regulation (GDPR) and other relevant privacy laws ..	26
<b>G.</b>	<b>UOW Accountability .....</b>	<b>26</b>
34	Compliance with its privacy obligations .....	26
35	Responding to a Data Breach .....	27
36	Training and Education .....	27
37	Roles & Responsibilities .....	28
<b>H.</b>	<b>Privacy Contacts .....</b>	<b>29</b>
38	Internal Contacts .....	29
39	External Contacts .....	29
<b>I.</b>	<b>Version Control Table .....</b>	<b>30</b>



## A. Privacy management plan overview

### 1 Introduction / Background

1. The University of Wollongong (“UOW”) has an obligation to manage Personal and/or Health information in compliance with the NSW *Privacy and Personal Information Protection Act 1998* (“PPIPA”) and the NSW *Health Records and Information Privacy Act 2002* (“HRIPA”), which may include regulations, statutory guidelines, codes of practice and privacy directions made under those Acts.
2. This Privacy Management Plan (PMP) has been produced in compliance with section 33 of PPIPA. A copy of this PMP will be provided to the Privacy Commissioner as soon as practicable after it is prepared and whenever it is amended, in compliance with section 33(5) of PPIPA.
3. This PMP operates as a UOW procedure document supporting UOW’s Privacy Policy and is to be read in conjunction with UOW’s Privacy Policy. All Staff and Affiliates must comply with UOW’s Privacy Policy and this PMP.
4. UOW’s Privacy Policy and this PMP can be found on UOW’s [Policy Directory](#) and [Privacy Homepage](#) located on the UOW website at <https://www.uow.edu.au/privacy/>. Any requests for hard copies of these documents can be directed to the Information Compliance Unit. See [Section 38](#) for contact details.
5. This PMP does not apply to UOW’s Related entities or any other agencies. UOW’s Related entities have their own policies and procedures for the management of Information provided to or collected by them.

### 2 Purpose

1. The purpose of this PMP is to outline:
  - a. how UOW complies with PPIPA and HRIPA when carrying out its functions and activities;
  - b. how UOW disseminates its policies and practices regarding privacy within UOW;
  - c. how an individual may request access or amendment to their Personal or Health information; and
  - d. how an individual may make a complaint or lodge a request for a formal review of UOW’s conduct if they consider their privacy may have been breached.
2. In certain circumstances, UOW may be subject to obligations under other privacy laws. Some of the circumstances where other privacy laws may apply in the exercise of UOW’s functions and activities are discussed in the following sections:
  - a. [Section 32](#) provides details of the application of the *Privacy Act 1988* (Cth); and
  - b. [Section 33](#) provides details of the application of the *(EU)General Data Protection Regulation 2016/679* (GDPR) and other applicable foreign laws.
3. Enquiries regarding the application of other relevant privacy laws may be directed to a UOW Privacy Officer. Refer to [Section 38](#) for contact details of UOW’s Privacy Officers.



### 3 Definitions

Word/Term	Definition (with examples if required)
Affiliate	Includes people holding University of Wollongong Honorary Awards as conferred by the University Council, including the awards of Emeritus Professor, Honorary Doctor and University Fellow; people appointed in accordance with the University's Appointment of Visiting and Honorary Academics Policy; and people engaged by the University as agency staff, contractors, volunteers and work experience students.
Health information	Health information, for the purpose of this policy, refers to health information defined in HRIPA (or as amended in HRIPA from time to time) as:  “(a) personal information that is information or an opinion about: (i) the physical or mental health or a disability (at any time) of an individual, or (ii) an individual's express wishes about the future provision of health services to him or her, or (iii) a health service provided, or to be provided, to an individual, or (b) other personal information collected to provide, or in providing, a health service, or (c) other personal information about an individual collected in connection with the donation, or intended donation, of an individual's body parts, organs or body substances, or (d) other personal information that is genetic information about an individual arising from a health service provided to the individual in a form that is or could be predictive of the health (at any time) of the individual or of any sibling, relative or descendant of the individual, or (e) healthcare identifiers”
Information	Health information and/or Personal information as the context permits.
Investigative agency	Investigative agencies are as defined in PPIPA and/or HRIPA as the context applies. These may include (but are not limited to) the Ombudsman's Office, the Independent Commission Against Corruption, the Law Enforcement Conduct Commission, the Health Care Complaints Commission, the Australian Health Practitioners Regulation Agency, the Anti-Discrimination Board and the Children's Guardian.
Law enforcement agency	As defined in PPIPA and/or HRIPA as the context applies.  Law enforcement agencies include the Police Force of NSW or of another State or Territory, the NSW Crime Commission, the Australian Federal Police, the Australian Crime Commission, the Director of Public Prosecutions of NSW, another State or Territory or the Commonwealth, the Department of Justice and/or the Office of the Sheriff of NSW.
Personal information	Personal information, for the purpose of this policy, refers to personal information defined in PPIPA (or as amended in PPIPA from time to time) as:



	<p>“Information or an opinion (including information or an opinion forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion.”</p> <p>Under PPIPA, personal information does not include:</p> <ol style="list-style-type: none"><li>information regarding an individual who has been deceased for more than 30 years;</li><li>information about an individual that is readily available in a publicly available publication; and</li><li>information or an opinion about an individual’s suitability for appointment or employment as a public sector official.</li></ol>
Privacy Impact Assessment Tool (PIA Tool)	<p>A tool that facilitates the identification and examination of privacy impacts associated with a UOW program, activity, or technology including consideration of the steps required to minimize privacy risks.</p> <p>The use of the PIA Tool aims to achieve best practice privacy compliance, protect UOW’s reputation and meet community standards.</p>
Related entities	UOW Global Enterprises, UOW Pulse and the Illawarra Health and Medical Research Institute (IHMRI).
Sensitive information	A subclass of Personal information relating to an individual's ethnic or racial origin, political opinions, religious or philosophical beliefs, trade union membership or sexual activities.
Staff	All people employed by the University including conjoint appointments, whether on continuing, permanent, fixed term, casual or cadet or traineeship basis.

#### 4 The Information Protection Principles and Health Privacy Principles

1. The Information Protection Principles (IPPs) that apply to public sector agencies such as UOW are contained in sections 8-19 of PPIPA.
2. The Health Privacy Principles (HPPs) that apply to UOW are contained in Schedule 1 of HRIPA.
3. The application of the IPPs and HPPs at UOW are discussed in this PMP. In limited circumstances, exemptions in PPIPA or HRIPA may allow UOW to not comply with the IPPs or the HPPs. Some of these circumstances are explained in this PMP where relevant to UOW.
4. Privacy codes of practice and public interest directions can modify the application of the IPPs or the HPPs. There are currently no codes of practice or public interest directions that are relevant to UOW’s management of Information.
5. UOW’s [Information Sheet - Privacy](#) provides a summary of the IPPs and HPPs and has been produced to assist Staff and Affiliates understand the requirements of each of the principles.
6. When developing or reviewing projects, programs or policies that involve the collection and handling of Personal or Health information, Staff and Affiliates are to consider the requirements



of the IPPs and HPPs, as discussed in this PMP. UOW's [PIA Tool](#) is available to assist Staff and Affiliates in the consideration and assessment of each of the privacy principles.

7. A UOW Privacy Officer should be consulted when considering the application of any exemptions to the IPPs or HPPs or when working through the [PIA Tool](#).

## **B. Collection of Information**

### **5 UOW must collect information for lawful purposes**

1. IPP 1 and HPP 1 state that UOW must not collect Information unless:
  - a. the Information is collected for a lawful purpose that is directly related to a UOW function or activity; and
  - b. the collection of the Information is reasonably necessary for that purpose.
2. If Information received by UOW is unsolicited (not actively collected by UOW), the principles relating to collection do not apply. However, if UOW decides to make use of, or take any action in relation to the unsolicited Information, then UOW is regarded to have 'collected' the Information and the collection principles will then apply. If UOW decides to keep any unsolicited Information, UOW will apply the provisions of PPIPA and HRIPA relating to the storage, use and disclosure of that Information.

### **6 How UOW determines the lawful purposes of collection**

1. In considering what lawful purposes might be 'directly related to a UOW function or activity', as required by IPP 1 and HPP 1, UOW will have regard to the objects and functions of UOW as set out in the *University of Wollongong Act 1989* (NSW). Examples of the purposes for which Information is collected and used by UOW include:
  - a. services and activities related to education delivery;
  - b. administration and management of students (from recruitment through to conferring of degrees and other awards);
  - c. research;
  - d. marketing and fundraising activities;
  - e. community engagement and promotion of UOW events and programs (including potential staff and students, alumni, donors and community groups, other industries);
  - f. quality improvement and planning activities (which may include surveys and competitions);
  - g. news and updates (which may include marketing strategies);
  - h. management of Staff and Affiliates including selection, employment, appraisal and remuneration;
  - i. student accommodation;
  - j. support services such as counselling/disability services;
  - k. scholarship opportunities; and
  - l. managing grievances, complaints or disputes.



## **7 UOW must collect Information directly from the individual**

1. IPP 2 and HPP 3 state that UOW must, when collecting Information, collect the Information directly from the individual to whom the Information relates, unless:
  - a. the individual authorised collection of the Personal information from someone else; or
  - b. the Personal information is provided by a parent or guardian of a person who is under the age of 16 years; or
  - c. it is unreasonable or impracticable to collect health information directly. An example of this may include where an individual lacks the capacity to provide their Health information due to health reasons, in which case that Health information may be collected from an authorised representative such as a carer or guardian.
2. Additionally, UOW may collect Information from third parties in accordance with exceptions to IPP 2 and HPP 3. An exception that may apply to UOW includes where indirect collection is otherwise lawfully authorised or required.

## **8 How UOW collects Information directly from the individual**

1. UOW collects Information directly from individuals, including:
  - a. prospective or current Staff and Affiliates;
  - b. prospective students or enrolled students;
  - c. alumni; and/or
  - d. members of the public interacting with UOW. An example of this may include a client of UOW's Northfields Clinic.
2. UOW facilitates the collection of Information directly from the individual through the provision of:
  - a. forms;
  - b. user-based electronic mail services for all Staff, Affiliates and students through a secure server;
  - c. secure web-based data collection systems via UOW's website; and/or
  - d. telephone and face-to-face interaction.
3. When dealing with an individual, UOW will require that individual to confirm their identity. This is to ensure that UOW is collecting Information directly from that individual to whom the Information relates. For example, the identity confirmation process may include sighting a government issued identification record or staff/student ID card. In instances where enquiries are received over the phone, UOW will use a three-point checklist prior to disclosing any Information.
4. UOW welcomes enquiries and actively seeks feedback (which may include via comments, compliments and complaints) from individuals. Information is collected and used to respond to any matters raised through the various communication systems, to improve UOW services and promote effective complaint handling processes.



## 9 Indirect collection of Information

1. At times, UOW collects Information indirectly, but only does so when UOW is lawfully authorised or required to do so, or where the individual has authorised collection from someone else. Circumstances where Information may be indirectly collected may include:
  - a. via surveillance cameras, lecture recordings or access logs (when attending or accessing UOW whether in person or virtual);
  - b. from Universities Admissions Centre (UAC), other tertiary institutions, UOW agents, student exchange partners and Related entities;
  - c. relevant government departments such as the Commonwealth government department with responsibility for immigration;
  - d. recruitment firms and employment agencies;
  - e. health care providers, in order to provide support services and adjustments to work or study;
  - f. individuals acting under the authority of the individual to whom the Information relates; or
  - g. where lawfully required by Law enforcement agencies or Investigative agencies.
2. Where Information is captured indirectly, UOW will make all reasonable efforts to notify affected individuals about UOW's intended handling of their Information, either by direct contact or via its policies, webpages, terms and conditions or other applicable methods. For example, UOW's [CCTV Surveillance Standard](#) provides details relating to UOW's handling of personal information collected via surveillance cameras. UOW's [Lecture Recording Procedures](#) provide details of Personal information that may be collected during the recording of lectures.
3. Where an individual authorises another person or organisation to collect Information on their behalf, UOW will require evidence of that authority in writing. This authority will be captured as a UOW record and managed in accordance with [UOW's Records Management Policy](#)

## 10 UOW must be open and transparent about the handling of Information

1. IPP 3 and HPP 4 state that if UOW collects Information from an individual, UOW must take all steps as are reasonable in the circumstances to ensure that, before the Information is collected or as soon as practicable after collection, the individual to whom the Information relates is made aware of the following ("Collection Statement" or "Privacy Statement"):
  - a. the fact that Information is being collected;
  - b. the purposes for which the Information is being collected;
  - c. all intended recipients of the Information;
  - d. whether the supply of the Information by the individual is required by law or is voluntary;
  - e. consequences for the individual if the Information (or any part of it) is not provided. For example, the provision of a particular service may not be possible if certain Information is not provided by the individual;
  - f. the existence of any right of access to, or correction of, the Information; and
  - g. the name and address of the agency that is collecting the Information and the agency that is to hold the Information. (For complete transparency, UOW will make all reasonable



efforts to provide details of where the Information is to be held, especially where it is to be transferred outside NSW).

2. Exceptions to IPP 3 and HPP 4 may apply to UOW in the following circumstances:
  - a. the collection is reasonably necessary for the purpose of research, or the compilation or analysis of statistics, in the public interest and it is unreasonable or impracticable for the Information to be collected directly from the individual to whom the Information relates; or
  - b. in the case of Health information (where the Health information was collected from someone else) making the individual aware of the collection of that Health information would pose a serious threat to the life or health of any individual. UOW will have regard to the guidelines issued under HRIPA when considering the application of exceptions to HPP4.
3. Where collection of Information is reasonably necessary for the purpose of research, researchers are required to submit an application to UOW's Human Research Ethics Committee (HREC). HREC oversees and assesses whether that collection is reasonable in the circumstances and whether the University's privacy obligations are addressed. UOW's dedicated Human Ethics webpage at <https://www.uow.edu.au/research-and-innovation/researcher-support/ethics/human-ethics/> provides further information.
4. In limited circumstances, UOW may apply the exceptions to IPP 3 and HPP 4 when responding to critical incidents. In these instances, it may be necessary to obtain relevant information from someone else other than the individual involved in the critical incident to ensure the safety of that individual or of any other individual.
5. UOW will consider the requirements of any other applicable legislation when collecting Information. Refer to [Section F](#) of this PMP for discussion of other applicable legislation.

## 11 UOW's use of Privacy Statements

1. UOW, including its faculties and business units, collects Information at different times and in varying ways. As part of that Information collection process, UOW will provide a Privacy Statement to the individual. Examples of the methods used by UOW to communicate Privacy Statements include:
  - a. targeted notices at the point of student admission/enrolment processes and employment application and acceptance processes,
  - b. notices within a form, a policy, an agreement or as part of terms and conditions (including student registration and employment terms and conditions);
  - c. notices when visiting the UOW website, via information delivery, instructions or FAQ's;
  - d. verbal communication where Information is collected by phone; or
  - e. signage, where Information is collected broadly and it is impracticable to provide individual Privacy Statements. Examples include areas under CCTV surveillance or filming of special occasions.
2. The [UOW Privacy Homepage](http://www.uow.edu.au/about/privacy/index.html) located at <http://www.uow.edu.au/about/privacy/index.html> provides links to some of UOW's various Privacy Statements, as their context applies:
  - a. Student Privacy and Disclosure Statement;



- b. Privacy Collection Statement for Recruitment and Employee Records;
  - c. Privacy Statement for UOW's alumni, donors and members of the community
  - d. MyUOW App privacy statement
  - e. UOW Learner Privacy Statement (Open Learning)
  - f. UOW Website Privacy Collection Statement.
3. UOW Privacy Officers provide guidance and assistance in the development of Privacy Statements and in the application of any exceptions to IPP 3 and HPP 4, where applicable.

## 12 UOW must ensure that Information collected is relevant to its lawful purpose

1. IPP 4 and HPP 2 state that if UOW collects Information from an individual, UOW must take such steps as are reasonable in the circumstances (having regard to the purposes for which the Information is collected) to ensure that:
  - a. the Information collected is relevant to that purpose, is not excessive (having regard to the purpose) and is accurate, up-to-date and complete; and
  - b. the collection of the Information does not intrude to an unreasonable extent on the personal affairs of the individual to whom the Information relates.
2. Staff and Affiliates are to consider the requirements of IPP 4 and HPP 2 when collecting Information from an individual. UOW's [PIA Tool](#) facilitates consideration and assessment of each of the privacy principles.
3. Where human participants are required for the purpose of research, UOW's Human Research Ethics Committee oversees and approves the intended research activity. HREC requires each researcher to outline the Information to be collected for the research project, assesses whether that collection is reasonable in the circumstances and determines whether the University's privacy obligations are addressed. UOW's dedicated Human Ethics webpage at <https://www.uow.edu.au/research-and-innovation/researcher-support/ethics/human-ethics/> provides further information.

## C. Management of Information by UOW

### 13 UOW must ensure security of Information

1. IPP 5 and HPP 5 state that if UOW holds Information it must ensure that:
  - a. the Information is kept for no longer than is necessary for the purposes for which the Information may lawfully be used;
  - b. the Information is disposed of securely and in accordance with any requirements for the retention and disposal of such Information;
  - c. the Information is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorized access, use, modification or disclosure, and against all other misuse; and
  - d. if it is necessary for the Information to be given to a person in connection with the provision of a service to UOW (third party engagement), everything reasonably within the power of UOW is done to prevent unauthorized use or disclosure of the Information.



## 14 UOW's commitment to protecting Information

1. UOW is committed to ensuring all business activities performed with the use of information technology systems are protected and maintained, and that sustainable procedures are in place to reflect best practice information technology security. UOW's [information technology policies](#) provide details of its commitment to the storage and protection of Information in compliance with its privacy obligations.
2. UOW's Data Governance Procedure, Data Quality Management Procedure and Data Handling Guidelines (available on UOW's [Policy directory](#)) provide the data governance framework relating to the availability, usability, integrity and security of all data held by UOW. This data includes Personal and Health information.
3. Staff and Affiliates are required to comply with UOW's [IT Acceptable Use Policy](#) and are expected to protect Information by ensuring that:
  - a. where appropriate, the [PIA Tool](#) is used to identify and minimize privacy risks prior to collecting and processing Personal or Health information;
  - b. records are stored in University approved systems (which have undergone an assessment of the system's security features);
  - c. access to systems or databases is restricted to those individuals with a legitimate business purpose;
  - d. systems that are password protected are appropriately utilised and managed; and
  - e. Information is destroyed securely e.g. hard copy records are placed in security destruction bins.
4. From time to time, Staff and Affiliates may be required to acknowledge their understanding of their compliance obligations in writing if handling certain high-risk categories of Information
5. In certain circumstances, as a security safeguard, UOW will remove identifiers before using Information in order to protect the privacy of that individual. For example, identifiers are removed from Information where UOW wishes to gain valuable insight for planning and/or research purposes.
6. Where UOW engages the services of a third party for the purpose of providing a particular service to UOW, all reasonable steps will be taken to ensure that the third party has robust practices in place to protect the Information and prevent its unauthorized use or disclosure. [Section 23](#) of this PMP provides further information on Third Party Engagement and Confidentiality.

## 15 UOW's recordkeeping obligations

1. UOW is subject to the *State Records Act 1998* (NSW), which requires UOW to comply with specific timeframes for the retention and disposal of documents. Once Information has reached its required retention period it is destroyed securely and in a compliant manner. UOW's [Records Management Policy](#) provides further information regarding the University's obligations under the *State Records Act 1998* (NSW).
2. In limited circumstances, UOW may decide to keep Information for a longer period than the period required for its original purpose. Where this is necessary, UOW will keep a record of its business decision regarding extended retention periods, where applicable.



## 16 UOW must check accuracy of Information before use

1. IPP 9 and HPP 9 state that if UOW holds Information, it must not use that Information without taking such steps as are reasonable in the circumstances to ensure that, having regard to the purpose for which the Information is proposed to be used, the Information is relevant, accurate, up to date, complete and not misleading.

## 17 How UOW ensures accuracy of Information before use

1. UOW will consider one or more of the following factors, as are reasonable on a case by case basis, to determine whether the Information it holds is relevant, accurate, up to date, complete and not misleading:
  - a. the purpose for which the Information was collected;
  - b. the sensitivity of the Information;
  - c. how many people have access to the Information;
  - d. the importance of accuracy to the proposed use;
  - e. the potential effects on the individual concerned if the Information is inaccurate, out-of-date or irrelevant;
  - f. the opportunities to subsequently correct the Information; and
  - g. the ease with which the Information can be checked.
2. Examples where UOW checks the accuracy of Information before use include:
  - a. checking student enrolment information such as visa and immigration status, pre-requisites and academic results;
  - b. checking prospective employee references, work history, academic qualifications and identification, as well as the employee's rights to work in Australia; and
  - c. checking Information provided in higher degree research (HDR) applications.

## 18 Use and Disclosure of Personal Information

1. In general terms, 'use' refers to the communication or handling of Information within UOW, whereas 'disclosure' refers to the communication or transfer of Information outside UOW, other than to the individual concerned. The principles relating to use and disclosure of Personal information are discussed below.
2. IPP 10 states that UOW must not use Personal information it holds for a purpose other than that for which it was collected unless:
  - a. the individual to whom the Personal information relates has consented to the use of the Personal information for that other purpose, or
  - b. the other purpose for which the Information is used is directly related to the purpose for which the Personal information was collected, or
  - c. the use of the Personal information for that other purpose is necessary to lessen or prevent a serious and imminent threat to any individual's health or safety, or the use is to assist in a stage of an emergency, and it is impracticable or unreasonable to seek the consent of the individual to whom the Information relates.



3. IPP 11 states that UOW must not disclose an individual's Personal information unless:
  - a. the individual concerned is reasonably likely to have been aware, or has been made aware at collection, that Personal information of that kind is usually disclosed to that other person or body; or
  - b. the disclosure is directly related to the purpose for which the Personal information was collected and UOW has no reason to believe that the individual concerned would object to the disclosure; or
  - c. the disclosure of the Personal information is necessary, on reasonable grounds, to prevent or lessen a serious and imminent threat to the life or health of any individual.
4. Exceptions to IPP 11 which may apply to UOW include where the disclosure of the Personal information concerned is:
  - a. made in connection with proceedings for an offence or for law enforcement purposes; or
  - b. authorised or required by subpoena, search warrant or other legal order; or
  - c. made to a Law enforcement agency for the purpose of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person; or
  - d. made to an Investigative agency as a result of an investigation from a complaint or other matter that was either made or referred from an Investigative agency or that could have been referred or made by UOW to the Investigative agency; or
  - e. the disclosure is necessary to assist in a stage of an emergency and it is impracticable or unreasonable to seek the consent of the individual to whom the Information relates.
5. IPP 12 states that UOW must not disclose Sensitive information without the consent of that individual unless the disclosure is necessary to prevent a serious and imminent threat to the health or safety of any person.

## 19 How UOW applies the use and disclosure principles of Personal information

1. Prior to collecting Information, UOW makes all efforts to identify the primary and directly related uses of that information and communicates the intended use and disclosure instances to individuals via a Privacy Statement (as discussed at [Section 11](#) above). As an example, during the enrolment process, students are informed of the various use/disclosure instances relating to their Information. Where a new or unrelated use is identified, UOW will seek the consent of the individual prior to proceeding unless an exemption applies.
2. Examples where UOW uses Personal Information for a purpose that is directly related to the primary purposes for which it was collected include:
  - a. provision of services to Students such as career support, study support;
  - b. responding to security/wellbeing concerns;
  - c. responding to work health and safety reports;
  - d. promotion of events and programs (including postgraduate study programs);
  - e. surveys and competitions;
  - f. quality improvement and planning;
  - g. handling of complaints and conducting investigations.



3. UOW's policies provide a mechanism through which UOW explains the various ways in which it uses and discloses Personal and/or Health information. For example, Personal information is managed by UOW for the purposes as set out in the [IT Acceptable Use Policy](#).
4. UOW applies learning analytics initiatives to student data in order to maximise each student's academic success and to support their student learning experience. This is achieved by giving each student, as well as authorised Staff and Affiliates, access to the student's learning-related information in order to build on that student's areas of strength, identify areas for improvement and to utilise support services offered by UOW. The use of analytics data involving students is governed by [UOW's Learning Analytics Data Use Policy](#).
5. UOW may also use analytics software and other business intelligence systems for quality and planning purposes. In these instances, Personal information may be used to develop the system intelligence. Where practicable, UOW will consider the use of non-identifiable data to achieve the purpose. The [PIA Tool](#) will also be utilised to consider all the relevant privacy principles and risk mitigation strategies.
6. Personal information may also be used and/or disclosed by UOW to manage emergency or crisis situations. This may include contacting individuals to provide important notices/updates relating to the emergency and/or disclosure of details to the relevant emergency service if required.
7. In limited circumstances UOW may use Personal information to exercise its duty of care responsibilities under the *Work Health and Safety Act 2011* (NSW) to ensure that UOW is a safe working and learning environment for Staff/Affiliates/Students and visitors.
8. Where Personal information is to be used for the purpose of undertaking research, UOW will refer to the [Statutory Guidelines on Research – 27B, Privacy and Personal Information Protection Act 1998 \(NSW\)](#). UOW's Human Research Ethics Committee (HREC) is responsible for approval of the research in accordance with the National Health and Medical Research Council (NHMRC) National Statement on Ethical Conduct in Human Research (2007). UOW's dedicated Human Ethics webpage at <https://www.uow.edu.au/research-and-innovation/researcher-support/ethics/human-ethics/> provides further information.
9. UOW welcomes enquiries and feedback (which includes comments, compliments and complaints) from the UOW community. In order to effectively manage and respond to enquiries and feedback UOW may need to share Personal information with specific units and Staff who are subject matter experts. Examples include Staff with expertise in records management, information technology, teaching and learning or human resources. Where reasonably practicable, the individual will be consulted prior to sharing the Personal information.
10. Where Personal information is used for direct marketing purposes, UOW will provide a clear mechanism through which an individual may choose to unsubscribe from receiving any further messages from UOW.
11. UOW may be required by law to disclose certain information. For example:
  - a. as part of mandatory reporting processes, UOW must disclose Personal information to various Government agencies. Examples are the Commonwealth government department with responsibility for immigration, the Commonwealth government department with responsibility for tertiary education and the Australian Taxation Office (ATO);



- b. under the *Public Interest Disclosures Act 1994* (NSW) or its equivalent, UOW may be obliged to make a disclosure regarding corruption, maladministration or other conduct governed by that Act;
  - c. as part of its mandatory notification obligations, UOW must disclose Personal information to certain Investigative agencies such as the Australian Health Practitioners Regulation Agency.
12. Where UOW receives a request or is authorised by law to disclose Personal information, UOW will:
- a. only disclose the Personal information that UOW is authorised to disclose under relevant legislation;
  - b. only provide the Personal information that falls within the scope of the request; and
  - c. keep a written record of the Personal information that has been disclosed.

UOW has developed the following Information Sheets to provide best practice guidance when responding to certain requests for information:

- [Information Sheet – Centrelink \(Human Services\) Inquiries](#) to assist staff to respond to requests for information from Human Services.
- [Requests for Student Conduct Reports by External Legal Admission Boards](#)

13. Where Personal information is to be disclosed to a Law enforcement agency, UOW will:
- a. only provide the Personal information that is relevant and necessary for the intended purpose;
  - b. obtain and document proof that the individual seeking the Personal information is a representative of the appropriate Law enforcement agency; and
  - c. keep a written record of the Personal information that has been disclosed.

UOW has developed an [Information Sheet – Requests for Information from Police](#) to assist Staff to respond to requests for information from police.

14. In some circumstances, taking into account the nature and context of a request received by a government agency (including a Law enforcement agency), UOW may refuse to comply in the absence of a subpoena, warrant or similar legal order. Where Personal information or Sensitive information is to be disclosed under a subpoena, warrant or similar legal order, UOW will:
- a. only provide the information that is within the scope of the order; and
  - b. keep a written record of the information that has been disclosed.

UOW has developed an [Information Sheet – Dealing with Subpoena Requests](#) to assist Staff and Affiliates to respond to requests for information under a subpoena.

15. In instances where Sensitive information is to be disclosed, UOW will always ensure that express consent is obtained from the individual. A record of the consent will be kept by UOW in accordance with its recordkeeping obligations. UOW will only depart from this practice in the circumstances permitted under PPIPA.
16. Where UOW engages a third party for the purpose of providing a service on behalf of UOW which involves use and/or disclosure of Personal information, UOW will manage that engagement in accordance with [Section 23](#) of this PMP.



17. UOW does not have any Memorandums of Understanding or referral arrangements with other agencies relating to the sharing of Personal information.

## 20 Use and Disclosure of Health Information

1. In general terms, 'use' refers to the communication or handling of Information within UOW, whereas 'disclosure' refers to the communication or transfer of Information outside UOW, other than to the individual concerned. The principles relating to use and disclosure of Health information are discussed below.
2. HPP 10 and HPP 11 state that UOW must not use or disclose Health information for another purpose (secondary purpose) other than the primary purpose for which it was collected unless:
  - a. the individual has provided consent;
  - b. the secondary purpose is directly related to the primary purpose and within the expectations of the individual;
  - c. it is reasonably believed to be necessary to lessen or prevent;
    - i. a serious and imminent threat to the life, health or safety of any person; or
    - ii. a serious threat to public health or public safety.
3. Exceptions to HPP 10 and HPP 11 which may apply to UOW include where the use and/or disclosure is:
  - a. made to a Law enforcement agency for law enforcement and related matters such as:
    - i. for the purposes of ascertaining the whereabouts of an individual who has been reported to police as a missing person, or
    - ii. where there are reasonable grounds to believe that an offence may have been, or may be, committed; or
  - b. lawfully authorised or required, or permitted under another law to do so, such as subpoena or search warrant; or
  - c. reasonably necessary to enable UOW to investigate or handle a complaint or other matter that may be referred or made to an Investigative agency, or that has been referred or made from an Investigative agency; or
  - d. necessary to be used by UOW as a part of its investigation, or in the reporting of its concerns to relevant persons or authorities, where UOW has reasonable grounds to suspect that:
    - i. unlawful activity has been or may be engaged in; or
    - ii. an individual has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the Health Practitioner Regulation National Law (NSW); or
    - iii. an individual has or may have engaged in conduct that may be grounds for disciplinary action such as a breach of UOW's Code of Conduct by Staff or Affiliates; or
  - e. reasonably necessary for the funding, management, planning or evaluation of health services, or for the training of UOW employees or persons working with UOW, or for research, or the compilation or analysis of statistics, in the public interest and;



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

- i. either the purpose cannot be served by de-identified Health information and it is impracticable to seek the consent of the individual for the use/disclosure, or reasonable steps are taken to de-identify the Health information; and
- ii. if it could reasonably be expected to identify individuals, the Health information is not published in a generally available publication; and
- iii. the use of the Health information is in accordance with the statutory guidelines issued under HRIPA by the Privacy Commissioner.

## 21 How UOW applies the use and disclosure principles of Health information

1. Prior to collecting Health information, UOW makes all efforts to identify the primary and directly related uses of that information and communicates the intended use and disclosure instances to individuals via a Privacy Statement (as discussed at [Section 11](#) above). For example, a student wishing to utilise support services such as counselling, or wishing to arrange reasonable adjustments, is required to register for the service and is provided with a Privacy Statement outlining how UOW will handle their Health information. Where a new or unrelated use is identified, UOW will seek the consent of the individual prior to proceeding.
2. UOW may be required by law to disclose Health information. This may include:
  - a. under search warrants, subpoenas, other legal orders or statutory instruments;
  - b. reporting of notifiable diseases pursuant to, for example, the *Public Health Act 2010* (NSW). Examples of notifiable diseases include, but are not limited to, Hepatitis A, B, C, D, E, Diphtheria, Tetanus, Pertussis and Tuberculosis.
3. Where UOW intends to use and/or disclose Health information for the purposes of providing training it will ensure that it complies with the [Statutory Guidelines on training – Health Records and Information Privacy Act 2002 \(NSW\)](#).
4. Where Health information is to be used for the purpose of undertaking research, UOW will refer to the [Statutory Guidelines on Research – Health Records and Information Privacy Act 2002 \(NSW\)](#). UOW's Human Research Ethics Committee (HREC) is responsible for approval of the research in accordance with the National Health and Medical Research Council (NHMRC) National Statement on Ethical Conduct in Human Research (2007). UOW's dedicated Human Ethics webpage at <https://www.uow.edu.au/research-and-innovation/researcher-support/ethics/human-ethics/> provides further information.
5. Where UOW intends to use Health information that may have been collected from a third party, UOW will ensure that it complies with the [Statutory guidelines on the collection of health information from a third party – Health Records and Information Privacy Act 2002 \(NSW\)](#).
6. UOW may verify and exchange a student's Health information with an external placement body for the purpose of clinical or other placement or practicum experience. UOW students are notified of this activity via a Privacy Statement in a relevant policy or via the subject outlines, as a requirement of a course of study. Examples of Health information that may be exchanged may include pre-existing medical conditions that could affect a student's placement activities and/or UOW's student personal accident insurance cover. In limited circumstances, where prior notification may not have been provided to the student (e.g via a Privacy Statement), disclosure of Health information will only occur with the consent of the student unless a lawful exception applies.
7. Where Health information is to be disclosed to a Law enforcement agency, UOW will:



- a. only provide the Health information that is relevant and necessary for the intended purpose;
- b. obtain and document proof that the person seeking the Health information is a representative of the appropriate Law enforcement agency;
- c. keep a written record of the Health information that has been disclosed.

UOW has developed an [Information Sheet – Requests for Information from Police](#) to assist Staff to respond to requests for information from police.

8. Where Health information is to be disclosed under a subpoena, warrant or similar legal order, UOW will:
  - a. only provide the Health information that is within the scope of the legal order; and
  - b. keep a written record of the Health information that has been disclosed.

UOW has developed an [Information Sheet – Dealing with Subpoena Requests](#) to assist Staff to respond to requests for information under a subpoena.

9. UOW may need to use Health information for the purpose of providing relevant student services. For example, a student may register with Disability Services as someone suffering a disability and it may be important for other areas of UOW to be aware of the student's condition, such as the Student Services Division, for arrangement of appropriate examination supervision. In these circumstances, this will be done with the consent of the student unless a lawful exception applies.
10. In limited circumstances UOW may use Health information to exercise its duty of care responsibilities under the *Work Health and Safety Act 2011* (NSW) to ensure that UOW is a safe working and learning environment for Staff/Affiliates/Students and visitors.
11. UOW welcomes enquiries and feedback (which includes comments, compliments and complaints) from staff, students and third parties. In order to effectively manage and respond to enquiries and feedback UOW may need to share Health information with specific units and Staff who are subject matter experts. Where reasonably practicable, the individual will be consulted prior to sharing the Health information.
12. UOW does not have any Memorandums of Understanding or referral arrangements with other agencies relating to the sharing of Health information.

## 22 Other Health Privacy Principles

1. HPP 12 – Identifiers

UOW does not assign unique identifiers for the management of Health information. However, UOW students are issued with a student number, which is a unique personal identifier, to facilitate efficient and effective student management.

2. HPP 13 – Anonymity

Wherever it is lawful and practicable, UOW will give individuals the opportunity to not identify themselves when entering into transactions with or receiving health services from UOW.

3. HPP 15 – Linkage to Health Records

UOW does not use a health records linkage system. In the event that a health linkage system is to be used by UOW, it will only do so with the individual's express consent.



## 23 Third Party Engagement and Confidentiality

1. Where UOW proposes to share particular Information with a contractor, agent or consultant engaged to undertake work for/with UOW (third party), UOW will take reasonable steps to ensure that the service provider has adequate measures in place to manage the Information in accordance with UOW Privacy Policy and this PMP. The [PIA Tool](#) is to be used by the relevant UOW business unit to assess the impact on any Information associated with the project or program that relates to the engagement.
2. If UOW transfers Information to a third party who is in a jurisdiction outside NSW or to a Commonwealth agency, UOW will do so on the following grounds:
  - a. the recipient must be subject to principles that are substantially similar to the NSW IPPs and HPPs; or
  - b. with the consent of the individual; or
  - c. the transfer is necessary for the performance of a contract in the interest of the individual between UOW and a third party; or
  - d. the transfer is necessary to lessen or prevent a serious and imminent threat to the life or health of the individual or another person (or to lessen or prevent a serious threat to public health or public safety); or
  - e. the transfer is otherwise permitted or required by an Act (including an Act of the Commonwealth) or any other law.
3. Engagement of technology-based third party vendors is usually managed by UOW's Infrastructure Management and Technology Services (IMTS). IMTS is responsible for conducting due diligence for projects that involve the development and management of information and communication technology resources in response to research, teaching and business requirements.
4. To facilitate UOW's due diligence process, UOW has created a questionnaire document, Data Privacy Questions for Third Party Suppliers. This document is given to third party suppliers to complete prior to engagement so that UOW has a clear understanding of a potential supplier's privacy practices.
5. In addition, cloud-based third party suppliers are also required to complete the Higher Education Cloud Vendor Assessment Tool. This tool poses key questions to facilitate assessment of cloud services provisioning, information security and data protection.
6. UOW will take all reasonable steps to include provisions in its contracts with third party suppliers that the third party:
  - a. is to comply with PPIPA and/or HRIPA or principles that are substantially similar to PPIPA and/or HRIPA;
  - b. must treat all data (whether provided by UOW, uploaded by users or generated by any applicable software) in a confidential manner and only use Information for the sole purpose for which it was provided to the third party;
  - c. must minimise opportunities for misuse of the Information, such as restricting access to the Information by its employees and/or contractors; and



- d. is to comply with UOW's recordkeeping requirements. For example, this may include retention requirements, disposal and/or return of the Information to UOW once the service is completed.
7. UOW has developed an [Information Sheet – Data Security and Third Party Engagement](#) which outlines key considerations when negotiating agreements with third party suppliers.

## 24 Public Registers Held by UOW

1. PPIPA requires agencies with responsibilities for public registers to comply with certain requirements.
2. A public register is defined in PPIPA as:  
“A register of personal or health information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)”.
3. UOW does not hold or manage any public registers as defined in PPIPA. However, UOW makes the following registers available on its website:
  - a. A contracts register as part of its *Government Information Public Access Act 2009* (NSW) mandatory disclosure obligations, available at <https://gipa.uow.edu.au/gipa/contract/allContracts> and
4. A register known as the graduate roll comprising the names of graduates and the courses conferred by UOW each year available at: <https://www.uow.edu.au/student/graduation/graduate-roll/>. Students provide consent for their details to be made publicly available on the graduate roll when applying to graduate. An individual who no longer wishes to have their Personal information accessible on UOW's public register may contact Student Central on 1300 275 869 or email [askuow@uow.edu.au](mailto:askuow@uow.edu.au).

## D. Rights to access/amend Information held by UOW

### 25 Access to Information Held by UOW

1. IPP 6 and 7 and HPP 6 and 7 state that if UOW holds Information:
  - a. it must take such steps as are, in the circumstances, reasonable to enable an individual to ascertain:
    - i. whether UOW holds Information relating to that individual;
    - ii. if UOW holds Information relating to that individual:
      - the nature of that Information;
      - the main purpose for which the Information is used; and
      - the individual's entitlement to gain access to the Information;
  - b. it must provide the individual with access to the Information without excessive delay or excessive expense.

### 26 How Information can be accessed from UOW

1. The rights to access/amend Information relate to an individual's own records.



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

2. UOW is committed to responding to requests for access to an individual's Information in a timely manner. The time taken by UOW to provide access to the Information will depend on the volume and nature of the request but all reasonable efforts will be made to provide access within 30 days.
3. Enquiries and requests for access to Information should be directed as follows:
  - a. Staff and Affiliates who wish to obtain access to their employment records should contact UOW's Human Resources Helpdesk via Unified or by phoning 4221 5902;
  - b. Students who wish to obtain access to their student records should contact Student Services Central on 1300 275 869 or email [askuow@uow.edu.au](mailto:askuow@uow.edu.au);
  - c. Higher degree research (HDR) students who wish to obtain access to their HDR student records should contact the Graduate Research School at <http://www.uow.edu.au/research/grs/index.html>;
  - d. All other enquiries can be made to [icu-enquiry@uow.edu.au](mailto:icu-enquiry@uow.edu.au).
4. In most instances, UOW will provide access to an individual's Information without a fee. However, there are some instances where a fee may be charged, such as where UOW provides an individual with their official UOW academic transcript.
5. An individual who is not satisfied with UOW's response to a request to access their Information may lodge a complaint or request a formal internal review (see [Section 29](#) Complaints and/or Internal Reviews).
6. An individual also has a right to access Information under the *Government Information (Public Access) Act 2009* (NSW). Lodgement and processing fees are payable using this method of access. Further details can be found on UOW's dedicated Access to Information webpage at <https://www.uow.edu.au/about/governance/access-to-information/>.
7. Where an individual seeks access to Information about another individual, this type of request will be managed in accordance with the disclosure principles (and any related exceptions) discussed at [section 18](#) and [section 20](#) of this PMP or alternatively the individual will be referred to UOW's Access to Information webpage.

## 27 Alteration of Information held by UOW

1. IPP 8 and HPP 8 state that:
  - a. where UOW holds Information, it must, at the request of the individual to whom the Information relates, make appropriate amendments (whether by way of corrections, deletions or additions) to ensure that the Information:
    - i. is accurate; and
    - ii. having regard to the purpose for which the Information was collected (or is to be used) and to any purpose that is directly related to that purpose, is relevant, up to date, complete and not misleading;
  - b. if UOW is not prepared to amend Information in accordance with a request by the individual to whom the Information relates, UOW must, if requested by the individual concerned, take such steps as are reasonable to attach to the Information any statement provided by that individual of the amendment sought, in such a manner that it is capable of being read with the Information;



- c. if Information is amended in accordance with this principle, the individual to whom the Information relates is entitled, if it is reasonably practicable, to have recipients of that Information notified of the amendments made by UOW.

## 28 How UOW handles requests for amendments to Information

2. UOW holds Information in a variety of systems for UOW lawful purposes.
3. Individuals may lodge a request to amend their Information as per the process outlined in Section 26.3 above.
4. Any requests for amendments must be accompanied by supporting evidence, which demonstrates that the Information is inaccurate or misleading, and the individual must be able to verify their identity when submitting the request. For example, the verification process may include sighting a government issued identification record or staff/student ID card.
5. Where Information held by UOW is amended, UOW will notify the recipients of that Information of the amendment, so far as it is reasonably practicable. The following factors will be taken into account on a case by case basis when determining whether it is reasonably practicable to notify others of the amendment:
  - a. who the recipients of the Information are;
  - b. the purpose for which the Information was collected;
  - c. the sensitivity of the Information;
  - d. the importance of the accuracy of the Information;
  - e. the potential effects on the individual concerned if the Information is inaccurate, out of date or irrelevant;
  - f. any future opportunities to correct inaccuracies before the Information is used; and
  - g. the ease and associated costs of notifying recipients.
6. UOW may refuse to amend Information it holds in certain circumstances, such as:
  - a. the change conflicts with UOW legislative obligations, or with university governance or business requirements. For example, UOW will not retrospectively change records of decisions where the Information was considered up to date at the time the decision was made;
  - b. the Information is a university business decision and is not deemed inaccurate by UOW; or
  - c. insufficient evidence has been provided to support the change.
7. Where UOW decides to refuse to amend the Information it holds, UOW will, where practicable (depending on the capabilities of the system used), attach a note to that Information of the amendment or addendum sought and UOW's reasons for its decision to refuse to amend the Information.

## E. Rights to raise concerns and/or make complaints

### 29 Complaints and/or Internal Reviews

1. UOW encourages individuals who have privacy concerns or complaints to contact one of UOW's Privacy Officers in the first instance so that, where possible, issues may be resolved



quickly and simply through informal means and/or general complaint handling procedures. Individuals are also entitled to seek a formal review of UOW's conduct ("Internal Review").

2. In the event a complaint or concern cannot be resolved informally, the individual's right to lodge an Internal Review will not be affected.
3. Information on how to contact a UOW Privacy Officer can be found in the Roles and Responsibilities section of this PMP or on UOW's privacy homepage at <http://www.uow.edu.au/about/privacy/index.html>.
4. A request for Internal Review can only be made where it is alleged that UOW's conduct has:
  - a. breached any of the Information Protection Principles in PPIPA or any of the Health Privacy Principles in HRIPA; or
  - b. breached a privacy code of practice that applies to UOW; or
  - c. disclosed Personal information kept in a public register.
5. An individual also has the right to contact the [Information and Privacy Commission NSW](#) to discuss any concerns relating to privacy or to make a complaint about UOW's conduct. Where a concern relates to UOW's alleged conduct referred to in 4a-4c above, the Privacy Commissioner may recommend that it would be more appropriate for an Internal Review application to be made.

### 30 The Internal Review process

1. Individuals are entitled to seek a formal review of UOW's conduct by submitting an application for an Internal Review. An application for Internal Review should:
  - a. be in writing;
  - b. be addressed to UOW;
  - c. specify a return address in Australia; and
  - d. be lodged with a UOW Privacy Officer within 6 months of the date the applicant first became aware of the alleged conduct. UOW may exercise its discretion to accept an application which is received after the end of the 6 month period.
2. Individuals can use the [Privacy Complaint Internal Review Application Form](#), available on UOW's privacy homepage, to make an application for an Internal Review.
3. The Internal Review will be conducted by a UOW Privacy Officer without any conflict of interest and/or involvement in the conduct which is the subject of the application.
4. Internal Reviews will be conducted in accordance with the requirements of Part 5 of PPIPA and with regard to any guidance produced by the NSW Privacy Commissioner. This includes the 'Internal Review Checklist for the Respondent Agency' published by the [Information and Privacy Commission NSW](#).
5. On receiving an application for an Internal Review UOW will, as soon as practicable, inform the [Information and Privacy Commission NSW](#) of the complaint and provide that office with a copy of the Internal Review application. The [Privacy Commissioner](#) will be kept informed of the outcome of the Internal Review and any action UOW proposes to take as a result of the Internal Review.



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

6. The Privacy Officer authorized to deal with the Internal Review (the reviewing officer) will assess the application and inform the applicant in writing of the following:
  - a. the name, title and contact details of the reviewing officer;
  - b. the reviewing officer's understanding of the conduct complained about and the privacy principle/s at issue;
  - c. that UOW is conducting the review under PPIPA or HRIPA, as appropriate;
  - d. the reviewing officer's suitability to deal with the matters raised by the application;
  - e. the required completion date for the review process (maximum of 60 days);
  - f. that an external review may be lodged with the [NSW Civil and Administrative Tribunal](#) (NCAT) if the review is not completed within the required timeframe; and
  - g. that the [Information and Privacy Commission NSW](#) will be kept informed of the progress and findings of the Internal Review.
7. UOW will consider any relevant material submitted by the applicant or by the Information and Privacy Commission NSW during the Internal Review.
8. Once the Internal Review has been completed, the reviewing officer, on behalf of UOW, may do one or more of the following:
  - a. take no further action on the matter;
  - b. make a formal apology to the applicant;
  - c. take such remedial action as it thinks appropriate;
  - d. provide undertakings that the conduct will not occur again; and/or
  - e. implement administrative measures to ensure that the conduct will not occur again.
9. Within 14 days of the completion of the Internal Review, the reviewing officer on behalf of UOW, will notify the applicant in writing of:
  - a. the findings of the Internal Review (and the reasons for those findings);
  - b. the action proposed to be taken by UOW (and the reasons for taking them); and
  - c. the right of the individual to have those findings, and the proposed action, reviewed by the [NSW Civil and Administrative Tribunal](#).

### 31 How to lodge an appeal of UOW's Internal Review decision

1. An applicant who has lodged an Internal Review application is entitled to seek a review by the [NSW Civil and Administrative Tribunal](#) of the conduct complained about if:
  - a. the applicant is not satisfied with the findings of the Internal Review; or
  - b. the applicant is not satisfied with the proposed actions to be taken by UOW; or
  - c. UOW has not dealt with the Internal Review application within the required 60 day timeframe.



## F. Application of other privacy laws

### 32 Application of Commonwealth Privacy Act

1. UOW is a statutory corporation established under the *University of Wollongong Act 1989* (NSW), and as such, is not an agency that falls within the scope of the *Privacy Act 1988* (Cth).
2. However, in some circumstances, Information handled by UOW may be expressly governed by the *Privacy Act 1988* (Cth). These circumstances may include:
  - a. where UOW collects tax file numbers from students, Staff and Affiliates;
  - b. via UOW's contractual interactions with Commonwealth funding agencies;
  - c. through UOW's IT service delivery to its Related entities; and
  - d. to meet compliance obligations under relevant Commonwealth legislation such as the Higher Education Support Act 2003 (Cth) relating to Commonwealth assistance to students.
3. The *Privacy (Australian Government Agencies – Governance) APP Code 2017*, (Code), requires all Australian Government agencies (as defined by s 5 of the Code) to have a designated Privacy Officer and a designated Privacy Champion.

### 33 Application of General Data Protection Regulation (GDPR) and other relevant privacy laws

1. The *(EU)General Data Protection Regulation 2016/679* (GDPR) and other applicable foreign laws may apply in certain circumstances, in relation to UOW's functions and activities. For example:
  - a. the GDPR, which extends its territorial scope outside the European Union (EU), may apply to UOW where it either has an establishment in the EU or offers goods and services or monitors the behaviour of individuals in or from the EU;
  - b. China's *Personal Information Protection Law* also extends its territorial scope to the processing of an individual's personal information outside of China, where products or services are provided to individuals in or from China;
2. UOW has developed an [Information Sheet-UOW and the EU General Data Protection Regulation \(GDPR\)](#) to assist its Staff and Affiliates to comply with the key principles of the GDPR;
3. Where the GDPR applies to any third party engagement, UOW will seek to comply with the Standard Contractual Clauses as set forth by the provisions of the GDPR. The [Information Sheet – Data Security and Third Party Engagement](#) provides guidance specific to the application of the GDPR.

## G. UOW Accountability

### 34 Compliance with its privacy obligations

1. UOW is committed to transparency and accountability in respect of its obligations under PPIPA and HRIPA. It aims to educate members of the public on how it complies with PPIPA and HRIPA and sets out the rights of individuals as outlined in those Acts. UOW demonstrates its commitment to privacy compliance through:
  - a. UOW's Privacy Policy and PMP, which is endorsed and approved by UOW Council;



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

- b. a dedicated privacy webpage at <https://www.uow.edu.au/privacy/> which contains best practice advice and resources for Staff and Affiliates and provides important details regarding UOW's handling of an individual's Information (including rights of the individual);
    - c. a dedicated team of Privacy Officers, who provide specialized training and advice and seek to ensure best practice guidance is embedded into UOW functions and activities.
  2. UOW's Principal Privacy Officer (or delegate) may audit UOW's compliance with this PMP.
  3. A breach of UOW's Privacy Policy or this PMP by Staff or Affiliates may constitute misconduct pursuant to UOW codes, policies and guidelines and may be subject to disciplinary action.
  4. It is also an offence under PPIPA and HRIPA for current or former UOW Staff or Affiliates, as part of their employment, to:
    - a. intentionally disclose or use Information that they have accessed, unless it is for a lawful or authorised purpose; and/or
    - b. supply, by way of a bribe or other similar corrupt conduct, any Information about an individual to another individual.
  5. Refer to the Roles and Responsibilities section for further details.

### 35 Responding to a Data Breach

1. Where UOW becomes aware of a suspected, potential or actual data breach involving Personal information or Health information it will take appropriate steps to identify, address and mitigate the impacts of the breach.
2. UOW's [Data Breach Response Plan](#) sets out UOW's procedures for managing a data breach, including the considerations around notifying those persons whose privacy may be affected by the breach as well as reporting to the appropriate regulator where relevant.
3. Staff and Affiliates are expected to report data breaches to a UOW Privacy Officer at [icu-enquiry@uow.edu.au](mailto:icu-enquiry@uow.edu.au). UOW's Privacy Officer will provide assistance and guidance to work through UOW's [Data Breach Response Plan](#) and take appropriate action.
4. In some circumstances UOW may have mandatory data breach notification requirements under other relevant privacy laws. Decisions regarding notification will be assessed on a case by case basis in accordance with the UOW Data Breach Response Plan and the relevant privacy laws.

### 36 Training and Education

1. UOW is committed to providing a robust privacy training and education program for its Staff and Affiliates, which includes providing:
  - a. privacy training as part of its induction programs;
  - b. clear expectations within the employment agreements of Staff and Affiliates regarding privacy obligations;
  - c. access to a privacy homepage which contains a range of information and resources about privacy including a Privacy Awareness e-book, privacy statements in use by UOW, a privacy training video and FAQ section;
  - d. access to current and informative guidance documents and tools such as:



- i. [UOW's Privacy Policy](#);
  - ii. this Privacy Management Plan;
  - iii. [UOW's Privacy Information Sheet](#);
  - iv. UOW's [Privacy Impact Assessment \(PIA\) tool](#);
  - v. UOW's [Data Breach Response Plan](#); and
  - vi. various other Information Sheets and tools (available via the 'Resources for Staff' section on [UOW's privacy homepage](#));
- e. privacy education via newsletters, information sessions, workshops and online training modules;
  - f. privacy advice on a case by case basis to Staff and Affiliates.
2. UOW Privacy Officers are committed to keeping abreast of best practice approaches to privacy compliance via regular attendance at the NSW privacy practitioners' group meetings held quarterly and other relevant meetings /conferences held from time to time.

### 37 Roles & Responsibilities

1. UOW's designated Privacy Champion is the Deputy Vice-Chancellor (Strategy and Assurance) who must ensure that the following functions are carried out:
  - a. Promoting a culture of privacy within the agency that values and protects personal information;
  - b. Providing leadership within the agency on broader strategic privacy issues;
  - c. Ensuring that the agency's privacy management plan is regularly reviewed;
  - d. Providing regular reports to the agency's executive, including about any privacy issues arising from the agency's handling of personal information.
2. UOW's Privacy Officers are:
  - a. General Counsel as UOW's Principal Privacy Officer;
  - b. Senior Manager, Information Compliance Unit – as UOW's designated Privacy Officer and main contact for privacy;
  - c. Officers in the Information Compliance Unit.
3. The Privacy Officers are responsible for:
  - a. training and education, including the development of guidance documents and tools;
  - b. providing advice and making best practice recommendations to Staff and Affiliates on privacy issues;
  - c. assisting with the development of Collection Statements;
  - d. liaising with relevant regulatory agencies such as the Information and Privacy Commission NSW;
  - e. responding to privacy complaints and conducting Internal Reviews;
  - f. implementing and maintaining UOW's Privacy Policy and this Privacy Management Plan;



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

- g. ensuring UOW's privacy homepage at <https://www.uow.edu.au/privacy/> contains current, relevant and best practice privacy information; and
  - h. preparing mandatory reports relating to privacy.
4. All Staff and Affiliates are responsible for:
- a. complying with UOW's privacy obligations and practices as specified in its Privacy Policy, this Privacy Management Plan and UOW's Code of Conduct when managing Information;
  - b. attending training or completing online privacy training to ensure that the principles of privacy best practice are maintained when handling Information.

## H. Privacy Contacts

### 38 Internal Contacts

Privacy enquiries may be directed to the Information Compliance Unit

Phone: (02) 4221 4368

Email: [icu-enquiry@uow.edu.au](mailto:icu-enquiry@uow.edu.au)

Website: <https://www.uow.edu.au/privacy/>

Post: Level 1, Building 22, Northfields Avenue, University of Wollongong NSW 2522

### 39 External Contacts

#### NSW Privacy and Information Commission (IPC)

Phone: 1800 472 679

Email: [ipcinfo@ipc.nsw.gov.au](mailto:ipcinfo@ipc.nsw.gov.au)

website: [www.ipc.nsw.gov.au](http://www.ipc.nsw.gov.au)

Post: GPO Box 7011, Sydney NSW 2000

#### NSW Civil and Administrative Tribunal (NCAT)

Phone: 1300 006 228 or (02) 9377 5711

website: [www.ncat.nsw.gov.au](http://www.ncat.nsw.gov.au)

Post: Level 9, John Maddison Tower, 85-90 Goulburn Street, Sydney NSW 2000



## I. Version Control Table

Version Control	Date Effective	Approved By	Amendment
1	7 December 2012	University Council	New Privacy Management Plan
2	16 December 2016	Vice-Chancellor	Amendments including name change to UOW's related entity, UOW divisions and various government departments. Addition of various statements demonstrating UOW's application of the privacy principles and amendments to reflect change in legislation.
3	15 February 2019	University Council	Consequential amendments as a result of the rescission of the Access to Information Policy.
4	23 May 2022	Vice-Chancellor	Amendments to further demonstrate UOW's application of the privacy principles to its functions and activities, and presented in accordance with the IPC Checklist to meet best practice
5	31 March 2023	Vice-Chancellor	Addition of the role of Privacy Champion and associated functions. Consequential amendments following establishment of Information Compliance Unit